Q. Cybersecurity presents several challenges that impact both national security and individual privacy. Discuss the major challenges faced in cybersecurity today, including technological, human and organizational factors. Evaluate the implications of these challenges for protecting critical infrastructure and personal data, and suggest strategies to address these issues effectively.

Ans: Cybersecurity is the practice of protecting devices, networks etc. from cyber attacks. Cyberattacks usually aims to accessing, destroying sensitive information and demanding money from users.

Introduction can be better. you can further contextualize it

Challenges faced from Cybersecurity:

Briefly mention how cybersecurity affects both national security & indi. privacy

Technological

1. AI: Artificial Intelligence can be use creating and enhance malicious activities. AI become more sophisticated day by day which increases the threat more ~~rapidly~~.

Alternatively you can write → Ex- Ransomware cyber threats etc.

2. Data breach: This is a top cybersecurity threats. It can be caused by lack of resource monitoring and sensitive information not being stored properly.

Human

Insider threats

Lack of awareness

1. Phising: A major cybersecurity threat. Phising is responsible for 90% of data breaches.

2. Internet of Things: IOT is stealing of our private information. Digital platforms steals our data from

various sources and use them for their benefit.

Organizational

1. Ransomware: This is a malware attack, where attackers demand money for decrypting users devices.

Ex: Delhi AIIMS Attack.

2. Third party Exposure: Organizations gives a chunks of their workload to the third parties to reduce the cost and time of their works. Which increase vulnerability of the organization.

Implications of these challenges:

1. Rapidly Evolving Threat landscape: day by day the escalation of the cyberattacks are evolving and became more complex.
2. Lack of awareness: People are unaware of the cybersecurity and their consequences.
3. Lack of Enough funds: Especially small businesses don't have enough funds for the implementation of cybersecurity frameworks.
4. Skill Shortage: Many organizations struggle to get skilled workforce for managing cybersecurity related issues.

Strategies to address these challenges

1. Data back up and Recovering plans: Backing up of critical data and recovery plans can minimize the

impact of cyberattacks.

2. Security training and awareness: Train and create awareness among people can minimize the cyberattacks.

3. Develop a cybersecurity Framework: A comprehensive cybersecurity framework must be create to secure the devices from cyber attacks.

4. Government Investment in cybersecurity: Government also need to invest in the field of cybersecurity.

There are 2300 approximately cyber attacks and 72% databreaches in 2023 as compared to 2021. Which shows us the importance of cybersecurity and their ~~attacks~~ threats. We need to create a cybersecurity temperament among people.

The suggestion provided are relevant but somewhat generic. Provide more specific strategies ex- AI driven cyber defence solution, strengthening cybersecurity technological

Instead you can summarize by mentioning about multilayered approach that includes technology, policy edu, etc.

3.5